

A Family of Reversible BCH Codes

Shuxing Li, Cunsheng Ding, and Hao Liu

Abstract

Cyclic codes are an interesting class of linear codes due to their efficient encoding and decoding algorithms as well as their theoretical importance. BCH codes form a subclass of cyclic codes and are very important in both theory and practice as they have good error-correcting capability and are widely used in communication systems, storage devices and consumer electronics. However, the dimension and minimum distance of BCH codes are not known in general. The objective of this paper is to study the dimension and minimum distance of a family of BCH codes over finite fields, i.e., a class of reversible BCH codes.

I. INTRODUCTION

Throughout this paper, let p be a prime and let q be a power of p . An $[n, k, d]$ linear code C over $\text{GF}(q)$ is a k -dimensional subspace of $\text{GF}(q)^n$ with minimum (Hamming) distance d . A linear code C over $\text{GF}(q)$ is called a *linear code with complementary dual (in short, LCD)* if $C \cap C^\perp = \{\mathbf{0}\}$, where C^\perp denotes the dual of C .

An $[n, k]$ linear code C is called *cyclic* if $(c_0, c_1, \dots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$. By identifying any vector $(c_0, c_1, \dots, c_{n-1}) \in \text{GF}(q)^n$ with

$$c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} \in \text{GF}(q)[x]/(x^n - 1),$$

any code C of length n over $\text{GF}(q)$ corresponds to a subset of the quotient ring $\text{GF}(q)[x]/(x^n - 1)$. A linear code C is cyclic if and only if the corresponding subset is an ideal of the ring $\text{GF}(q)[x]/(x^n - 1)$.

Note that every ideal of $\text{GF}(q)[x]/(x^n - 1)$ is principal. Let $C = \langle g(x) \rangle$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the elements of C . Then $g(x)$ is unique and called the *generator polynomial*, and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check polynomial* of C . Let $f(x) \in \text{GF}(q)[x]$ be a polynomial with degree l , then the reciprocal polynomial of f is defined to be $f_R(x) = x^l f(x^{-1})$. f is called self-reciprocal if and only if $f(x) = f_R(x)$. A cyclic code C with generator polynomial $g(x)$ is called *reversible* if $g(x)$ is self-reciprocal. The reversibility implies if

$$(c_0, c_1, \dots, c_{n-1}) \in C,$$

then

$$(c_{n-1}, c_{n-2}, \dots, c_0) \in C.$$

It is easily seen that reversible cyclic codes are LCD codes.

Let $m \geq 1$ be a positive integer and let $n = q^m - 1$. Let α be a generator of $\text{GF}(q^m)^*$. For any i with $1 \leq i \leq q^m - 2$, let $m_i(x)$ denote the minimal polynomial of α^i over $\text{GF}(q)$. For any $2 \leq \delta < n$, define

$$g_{(q,m,\delta)}^+(x) = \text{lcm}(m_1(x), m_2(x), \dots, m_{\delta-1}(x)),$$

and

$$g_{(q,m,\delta)}^-(x) = \text{lcm}(m_{n-\delta+1}(x), m_{n-\delta+2}(x), \dots, m_{n-1}(x)).$$

S. Li is with the Department of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (E-mail: lsxlslslx1987@gmail.com).

C. Ding is with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (E-mail: cding@ust.hk).

H. Liu is with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (E-mail: hliuar@connect.ust.hk).

where lcm denotes the least common multiple of these minimal polynomials. Let $C_{(q,m,\delta)}$ denote the cyclic code of length n with generator polynomial $g_{(q,m,\delta)}^+(x)$. This code $C_{(q,m,\delta)}$ is called the *narrow-sense primitive BCH code with designed distance δ* . The codes $C_{(q,m,\delta)}$ have been studied in series of papers, including [1], [3], [4], [5], [7], [8], [9], [11], [12], [16], [18], [25]. However, the dimension and minimum distance of the codes $C_{(q,m,\delta)}$ are still open in general.

For any $2 \leq \delta < (n+2)/2$, define

$$\tilde{g}_{(q,m,\delta)}(x) = \text{lcm}(g_{(q,m,\delta)}^-(x), g_{(q,m,\delta)}^+(x)).$$

Let $\tilde{C}_{(q,m,\delta)}$ denote the cyclic code of length n with generator polynomial $\tilde{g}_{(q,m,\delta)}(x)$. $\tilde{C}_{(q,m,\delta)}$ is a reversible cyclic code which was studied by Massey for the data storage applications [19]. For the code $\tilde{C}_{(q,m,\delta)}$ with length n and minimum distance d , it was shown in [24] that

$$\begin{cases} d = \delta & \text{if } \delta \mid n, \\ d \geq \delta + 1 & \text{otherwise.} \end{cases}$$

Moreover, if we consider the even-like subcode of $\tilde{C}_{(q,m,\delta)}$, namely, the code $\overline{C}_{(q,m,\delta)}$ with length n and generator polynomial

$$\overline{g}_{(q,m,\delta)}(x) = (x-1)\tilde{g}_{(q,m,\delta)}(x),$$

its minimum distance is at least 2δ by the BCH bound. Hence, a potential great improvement on the minimum distance is expected by considering the even-like subcode of $\tilde{C}_{(q,m,\delta)}$. This intuition motivates us to study the code $\overline{C}_{(q,m,\delta)}$, which is a reversible BCH code.

Recently, LCD codes have found an important application in cryptography [6]. Moreover, it was shown that asymptotically good LCD codes exist [13], [20], [23]. These are our major motivations of studying reversible BCH codes, which are a special class of LCD codes. The objective of this paper is to study the fundamental parameters, namely dimensions and minimum distances of the reversible BCH codes $\overline{C}_{(q,m,\delta)}$.

II. THE DIMENSION OF THE REVERSIBLE BCH CODES $\overline{C}_{(q,m,\delta)}$

Our task in this section is to study the dimension of the codes $\overline{C}_{(q,m,\delta)}$. It is in general a hard problem to determine the dimension of a BCH code.

A. The dimension of $\overline{C}_{(q,m,\delta)}$ when δ is relatively small

In [9], the authors derived the dimension of the narrow-sense primitive BCH code $C_{(q,m,\delta)}$ when δ is relatively small. In this subsection, we develop similar results for the dimension of the reversible BCH code $\overline{C}_{(q,m,\delta)}$.

Any positive integer s with $0 \leq s \leq n$ has a unique q -ary expansion as $s = \sum_{i=0}^{m-1} s_i q^i$, where $0 \leq s_i \leq q-1$. We use C_δ to denote the q -cyclotomic coset in \mathbb{Z}_n containing δ , which is defined by

$$C_\delta = \{\delta q^i \bmod n : 0 \leq i \leq m-1\}.$$

We use $cl(\delta)$ to denote the coset leader of C_δ , which is the smallest integer in C_δ . The q -ary expansion sequence of $s = \sum_{i=0}^{m-1} s_i q^i$ is denoted as $\bar{s} = (s_{m-1}, s_{m-2}, \dots, s_0)$. Below, we simply call the q -ary expansion sequence of s as the sequence of s , whenever this causes no confusion. The weight of \bar{s} is defined to be the number of nonzero entries among \bar{s} and denoted by $wt(\bar{s})$. Define the support of \bar{s} as

$$\text{supp}(\bar{s}) = \{0 \leq i \leq m-1 \mid s_i \neq 0\}.$$

We have the following properties regarding q -cyclotomic cosets modulo $n = q^m - 1$.

Lemma 1. *Let $m \geq 2$ and $n = q^m - 1$. Then we have the following.*

- 1) When m is odd, for $1 \leq i \leq q^{(m+1)/2}$, $|C_i| = |C_{-i}| = m$. For $1 \leq i, j \leq q^{(m+1)/2}$, $j \in C_i$, or equivalently $-j \in C_{-i}$, if and only if

$$j \equiv q^l i \pmod{n}$$

for some $0 \leq l \leq m-1$.

- 2) When m is even, $|C_{q^{m/2}+1}| = |C_{-q^{m/2}-1}| = \frac{m}{2}$ and $|C_i| = |C_{-i}| = m$ for $1 \leq i \leq 2q^{m/2}$, $i \neq q^{m/2} + 1$. For $1 \leq i, j \leq 2q^{m/2}$, $j \in C_i$, or equivalently $-j \in C_{-i}$, if and only if

$$j \equiv q^l i \pmod{n}$$

for some $0 \leq l \leq m-1$.

Proof: 1) The proof is essentially the same as that of [9, Theorem 3] (see also [1, Lemmas 8,9]), and is omitted.

2) The proof is essentially the same as that of [9, Theorem 3], and is omitted. ■

Lemma 2. Let $m \geq 2$ and let $n = q^m - 1$. Then the following statements hold.

- 1) When m is odd, for $1 \leq i, j \leq q^{(m+1)/2}$, $-j \in C_i$ if and only if

$$\bar{i} = (0, \dots, 0, \underset{\frac{m-1}{2}}{q-1}, \dots, \underset{1}{q-1}, u),$$

$$\bar{j} = (0, \dots, 0, \underset{\frac{m-1}{2}}{q-1-u}, \underset{\frac{m-3}{2}}{q-1}, \dots, q-1),$$

or

$$\bar{i} = (0, \dots, 0, \underset{\frac{m-1}{2}}{q-1-u}, \underset{\frac{m-3}{2}}{q-1}, \dots, q-1),$$

$$\bar{j} = (0, \dots, 0, \underset{\frac{m-1}{2}}{q-1}, \dots, \underset{1}{q-1}, u),$$

where $0 \leq u \leq q-1$.

- 2) When m is even and $q > 2$, for $1 \leq i, j \leq 2q^{m/2}$, $-j \in C_i$ if and only if

$$\bar{i} = (0, \dots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \dots, q-1, q-2),$$

$$\bar{j} = (0, \dots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \dots, q-1, q-2),$$

or

$$\bar{i} = (0, \dots, 0, \underset{\frac{m}{2}-1}{q-1}, \dots, \underset{1}{q-1}, q-2),$$

$$\bar{j} = (0, \dots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \dots, q-1),$$

or

$$\bar{i} = (0, \dots, 0, \underset{\frac{m}{2}}{1}, \underset{\frac{m}{2}-1}{q-1}, \dots, q-1),$$

$$\bar{j} = (0, \dots, 0, \underset{\frac{m}{2}-1}{q-1}, \dots, \underset{1}{q-1}, q-2),$$

or

$$\bar{i} = (0, \dots, 0, \underset{\frac{m}{2}-1}{q-1}, \dots, q-1),$$

$$\bar{j} = (0, \dots, 0, \underset{\frac{m}{2}-1}{q-1}, \dots, q-1).$$

$$\bar{j} = (0, \dots, 0, \frac{1}{\frac{m}{2}}, \dots, 1),$$

or

$$\bar{j} = (0, \dots, 0, \frac{m}{2}-2, \dots, 1),$$

or

$$\bar{j} = (0, \dots, 0, \underbrace{1}_{\frac{m}{2}-1}, \dots, 1),$$

or

$$\bar{j} = (0, \dots, 0, \frac{1}{2}, \dots, 1, 0, 1),$$

or

$$\bar{j} = (0, \dots, 0, \frac{1}{2}, 0, 1, \dots, 1).$$

Proof: 1) If $-j \in C_i$, then there exists an l with $0 \leq l \leq m-1$, such that $q^l i + j \equiv 0 \pmod{n}$. Hence,

$$\overline{q^l i + j} = (q-1, q-1, \dots, q-1).$$

Since $m = wt(\overline{q^l i + j}) \leq wt(\bar{i}) + wt(\bar{j}) \leq m + 1$, we have $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m-1}{2}, \frac{m+1}{2}\}$ or $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m+1}{2}\}$. If $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m-1}{2}, \frac{m+1}{2}\}$, then clearly, $\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j}) = \emptyset$. Otherwise, if $\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j}) \neq \emptyset$, there is at least one entry in $\overline{q^l i + j}$, which is not $q - 1$. Hence, $\overline{q^l i}$ and \bar{j} must have the following two forms

$$\bar{j} = (0, \dots, 0, \underset{2}{q-1}, \dots, q-1),$$

or

$$\bar{j} = (0, \dots, 0, \underset{\frac{m-3}{2}}{q-1}, \dots, q-1),$$

If $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m+1}{2}\}$, then clearly, $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j})| \geq 1$. If $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j})| > 1$, then there is at least one entry in $\overline{q^l i + j}$, which is not $q-1$. Hence, $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j})| = 1$. Therefore, $\overline{q^l i}$ and \bar{j} must have the following $2q-4$ forms

$$\begin{aligned}\overline{q^l i} &= (q-1, \dots, q-1, u, 0, \dots, 0), \\ \overline{j} &= (0, \dots, 0, q-1-u, q-1, \dots, q-1),\end{aligned}$$

or

$$\begin{aligned}\overline{q^l i} &= (q-1, \dots, q-1, \underbrace{0}_{\frac{m+1}{2}}, \dots, 0, u), \\ \overline{j} &= (0, \dots, 0, q-1, \dots, q-1, \underbrace{q-1-u}_{\frac{m-1}{2}}),\end{aligned}$$

where $1 \leq u \leq q-2$. Therefore, the conclusion follows. \square

2) If $-j \in C_i$, then there exists an l with $0 \leq l \leq m-1$, such that $q^l i + j \equiv 0 \pmod{n}$. Hence,

$$\overline{q^l i + j} = (q-1, q-1, \dots, q-1).$$

Since $m = wt(\overline{q^l i + j}) \leq wt(\bar{i}) + wt(\bar{j}) \leq m + 2$, we must have

$$\{wt(\bar{i}), wt(\bar{j})\} = \begin{cases} \{\frac{m}{2} + 1\}, \text{ or} \\ \{\frac{m}{2}, \frac{m}{2} + 1\}, \text{ or} \\ \{\frac{m}{2} - 1, \frac{m}{2} + 1\}, \text{ or} \\ \{\frac{m}{2}\}. \end{cases}$$

If $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m}{2} + 1\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j})| = 2$. Hence, $\overline{q^l i}$ and \bar{j} must have the following form

$$\begin{aligned}\overline{q^i} &= (q-1, \dots, q-1, q-2, \underset{\frac{m}{2}+1}{0}, \dots, \underset{\frac{m}{2}-1}{0}, 1), \\ \overline{j} &= (0, \dots, 0, 1, \underset{\frac{m}{2}}{q-1}, \dots, \underset{\frac{m}{2}-1}{q-1}, q-2).\end{aligned}$$

If $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m}{2}, \frac{m}{2} + 1\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j})| = 1$. Hence, $\overline{q^l i}$ and \bar{j} must have the following two forms

$$\begin{aligned}\overline{q^l i} &= (q-1, \dots, q-1, q-2, 0, \dots, 0), \\ \overline{j} &= (0, \dots, 0, 1, q-1, \dots, q-1),\end{aligned}$$

or

$$\begin{aligned}\overline{q^i} &= (q-1, \dots, q-1, \underset{m-1}{0}, \dots, 0, 1), \\ \overline{j} &= (0, \dots, 0, \underset{\frac{m}{2}-1}{q-1}, \dots, \underset{1}{q-1}, q-2).\end{aligned}$$

If $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m}{2} - 1, \frac{m}{2} + 1\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j})| = 0$. Hence, there is at least one entry in $(q^l i + j)$ which is not equal to $q - 1$. If $\{wt(\bar{i}), wt(\bar{j})\} = \{\frac{m}{2}\}$, then $|\text{supp}(\overline{q^l i}) \cap \text{supp}(\bar{j})| = 0$. Hence, $\overline{q^l i}$ and \bar{j} must have the following form

$$\begin{aligned}\bar{i} &= (q-1, \dots, q-1, 0, \dots, 0), \\ \bar{j} &= (0, \dots, 0, q-1, \dots, q-1).\end{aligned}$$

Therefore, the conclusion follows.

3) The proof is similar to that of 2) and is omitted here. ■

As a consequence, we have the following proposition.

Proposition 3. *Let $m \geq 2$ and $n = q^m - 1$.*

1) *Suppose m is odd. Then*

$$|\{(cl(i), cl(j)) \mid -j \in C_i, 1 \leq i, j \leq l\}| \\ = \begin{cases} 0 & \text{if } 1 \leq l \leq q^{(m+1)/2} - q, \\ 2h & \text{if } l = q^{(m+1)/2} - q + h, 1 \leq h \leq q - 2, \\ 2(q - 1) & \text{if } q^{(m+1)/2} - 1 \leq l \leq q^{(m+1)/2}. \end{cases}$$

2) *Suppose m is even and $q > 2$. Then*

$$|\{(cl(i), cl(j)) \mid -j \in C_i, 1 \leq i, j \leq l\}| \\ = \begin{cases} 0 & \text{if } 1 \leq l \leq q^{m/2} - 2, \\ 1 & \text{if } q^{m/2} - 1 \leq l \leq 2q^{m/2} - 3, \\ 2 & \text{if } l = 2q^{m/2} - 2, \\ 4 & \text{if } 2q^{m/2} - 1 \leq l \leq 2q^{m/2}. \end{cases}$$

3) *Suppose m is even and $q = 2$. Then*

$$|\{(cl(i), cl(j)) \mid -j \in C_i, 1 \leq i, j \leq l\}| \\ = \begin{cases} 0 & \text{if } 1 \leq l \leq 2^{m/2} - 2, \\ 1 & \text{if } 2^{m/2} - 1 \leq l \leq 2^{(m/2)+1} - 4, \\ 3 & \text{if } 2^{(m/2)+1} - 3 \leq l \leq 2^{(m/2)+1} - 2, \\ 5 & \text{if } 2^{(m/2)+1} - 1 \leq l \leq 2^{(m/2)+1}. \end{cases}$$

Combining Lemma 1 and Proposition 3, we have the following theorem.

Theorem 4. *Let $m \geq 2$ and $n = q^m - 1$. Given an integer $2 \leq \delta \leq (n + 2)/2$, let δ_q and δ_0 be the unique integers such that $\delta - 1 = \delta_q q + \delta_0$, where $0 \leq \delta_0 < q$. Then the dimension k of the code $\overline{C}_{(q,m,\delta)}$ is given below.*

1) *When m is odd,*

$$k = \begin{cases} q^m - 2 - 2m(\delta_q(q - 1) + \delta_0) & \text{if } \delta \leq q^{(m+1)/2} - q, \\ q^m - 2 - 2m(q^{(m-1)/2} - 1)(q - 1) & \text{if } q^{(m+1)/2} - q + 1 \leq \delta \leq q^{(m+1)/2} + 1. \end{cases}$$

2) *When m is even and $q > 2$,*

$$k = \begin{cases} q^m - 2 - 2m(\delta_q(q - 1) + \delta_0) & \text{if } \delta \leq q^{m/2} - 1, \\ q^m - 2 - 2m(\delta_q(q - 1) + \delta_0 - \frac{1}{2}) & \text{if } q^{m/2} \leq \delta \leq q^{m/2} + 1, \\ q^m - 2 - 2m(\delta_q(q - 1) + \delta_0 - 1) & \text{if } q^{m/2} + 2 \leq \delta \leq 2q^{m/2} - 2, \\ q^m - 2 - 2m(\delta_q(q - 1) + \delta_0 - \frac{3}{2}) & \text{if } \delta = 2q^{m/2} - 1, \\ q^m - 2 - 2m(\delta_q(q - 1) + \delta_0 - \frac{5}{2}) & \text{if } 2q^{m/2} \leq \delta \leq 2q^{m/2} + 1. \end{cases}$$

3) *When m is even and $q = 2$,*

$$k = \begin{cases} 2^m - 2 - 2m(\delta_q + \delta_0) & \text{if } \delta \leq 2^{m/2} - 1 \text{ and } m \geq 4, \\ 2^m - 2 - 2m(\delta_q + \delta_0 - \frac{1}{2}) & \text{if } 2^{m/2} \leq \delta \leq 2^{m/2} + 1 \text{ and } m \geq 4, \\ 2^m - 2 - 2m(\delta_q + \delta_0 - 1) & \text{if } 2^{m/2} + 2 \leq \delta \leq 2^{(m/2)+1} - 3 \text{ and } m \geq 4, \\ 2^m - 2 - 2m(\delta_q + \delta_0 - 2) & \text{if } 2^{(m/2)+1} - 2 \leq \delta \leq 2^{(m/2)+1} - 1 \text{ and } m \geq 6, \\ 2^m - 2 - 2m(\delta_q + \delta_0 - 3) & \text{if } 2^{(m/2)+1} \leq \delta \leq 2^{(m/2)+1} + 1 \text{ and } m \geq 6. \end{cases}$$

In addition, the minimum distance d of the code satisfies that $d \geq 2\delta$.

Proof: Let $\bar{g}_{(q,m,\delta)}(x)$ be the generator polynomial of $\bar{C}_{(q,m,\delta)}$. For the dimension of the code, we only prove 2) since the proofs of 1) and 3) are similar. By 2) of Lemma 1, the degree of $\bar{g}_{(q,m,\delta)}(x)$ equals

$$1 + 2m(\delta_q(q-1) + \delta_0) - \varepsilon m - |\{(cl(i), cl(j)) \mid -j \in C_i, 1 \leq i, j \leq \delta-1\}|m,$$

where

$$\varepsilon = \begin{cases} 0 & \text{if } \delta \leq q^{m/2} + 1, \\ 1 & \text{if } \delta \geq q^{m/2} + 2. \end{cases}$$

Together with 2) of Proposition 3, we have

$$\deg(\bar{g}_{(q,m,\delta)}(x)) = \begin{cases} 1 + 2m(\delta_q(q-1) + \delta_0) & \text{if } \delta \leq q^{m/2} - 1, \\ 1 + 2m(\delta_q(q-1) + \delta_0 - \frac{1}{2}) & \text{if } q^{m/2} \leq \delta \leq q^{m/2} + 1, \\ 1 + 2m(\delta_q(q-1) + \delta_0 - 1) & \text{if } q^{m/2} + 2 \leq \delta \leq 2q^{m/2} - 2, \\ 1 + 2m(\delta_q(q-1) + \delta_0 - \frac{3}{2}) & \text{if } \delta = 2q^{m/2} - 1, \\ 1 + 2m(\delta_q(q-1) + \delta_0 - \frac{5}{2}) & \text{if } 2q^{m/2} \leq \delta \leq 2q^{m/2} + 1. \end{cases}$$

Therefore, the conclusion on the dimension in 2) follows. Moreover, by the BCH bound, $\bar{C}_{(q,m,\delta)}$ has minimum distance $d \geq 2\delta$. ■

Remark 1. For the code $\bar{C}_{(q,m,\delta)}$, if

$$\sum_{i=0}^{\delta} \binom{n}{i} (q-1)^i > q^{n-k}, \quad (1)$$

then $d \leq 2\delta$ by the sphere packing bound. Therefore, the knowledge on the dimension of the code $\bar{C}_{(q,m,\delta)}$ may provide more precise information on the minimum distance in some cases. As an illustration, we use Theorem 4 and the inequality (1) to get some binary codes $\bar{C}_{(2,m,\delta)}$ with $d = 2\delta$, which are listed in Table I.

TABLE I
SOME BINARY CODE $\bar{C}_{(2,m,\delta)}$ WITH $d = 2\delta$

m	δ
{5,6,7}	{3}
{8,9,10,11,12,13}	{3,5}
{14,15,17,17,18,19}	{3,5,7}
{20}	{3,5,7,9}

B. The dimension of $\bar{C}_{(q,m,\delta)}$ when $\delta = q^\lambda$ and $\frac{m}{2} \leq \lambda \leq m-1$

In [18], the dimension of the narrow-sense primitive BCH code $C_{(q,m,\delta)}$ with $\delta = q^\lambda$ is considered. The author derived two closed formulas concerning the dimension of such code. In this subsection, we use the idea in [18] to give an estimate of the dimension of the reversible BCH code $\bar{C}_{(q,m,\delta)}$ with $\delta = q^\lambda$, where $\frac{m}{2} \leq \lambda \leq m-1$.

Let s and r be two positive integers. Given a sequence of length s and a fixed integer a with $0 \leq a \leq q-1$, we say that the sequence contains a straight run of length r with respect to a , if it has r consecutive entries formed by a . If we view the sequence as a circle where the first and last entry are glued together, we say that the sequence contains a circular run of length r with respect to a , if this circle has r consecutive entries formed by a . When the specific choice of the integer a does not matter, we simply say that the sequence has a straight or circular run of length r . Clearly, a straight run is also a circular run and the

converse is not necessarily true. We use $l_r(s)$ to denote the number of sequences of length s , which contains a straight run of length r . Particularly, we define $l_r(0) = 0$. The following is a recursive formula of $l_r(s)$ which was presented in [18].

Proposition 5. [18, p. 155] *Let s and r be two nonnegative integers. Then*

$$l_r(s) = \begin{cases} 0 & \text{if } 0 \leq s < r, \\ 1 & \text{if } s = r, \\ ql_r(s-1) + (q-1)(q^{s-r-1} - l_r(s-r-1)) & \text{if } s > r. \end{cases}$$

Throughout the rest of this section, we always assume that $\delta = q^\lambda$ and $\frac{m}{2} \leq \lambda \leq m-1$. Recall that the narrow-sense BCH code $C_{(q,m,\delta)}$ has generator polynomial $g_{(q,m,\delta)}^+(x)$. Set $r = m - \lambda$. Note that $\delta - 1$ corresponds to following sequence

$$\overline{\delta - 1} = (\underbrace{0, \dots, 0}_r, \underbrace{q-1, q-1, \dots, q-1}_{\lambda-1}).$$

The key observation in [18] is that for $1 \leq i \leq n-1$, α^i is a root of $g_{(q,m,\delta)}^+(x)$ if and only if the sequence of i has a circular run of length at least r with respect to 0. Similarly, note that $n - \delta + 1$ corresponds to the following sequence

$$\overline{n - \delta + 1} = (\underbrace{q-1, \dots, q-1}_r, \underbrace{0, 0, \dots, 0}_{\lambda-1}).$$

Therefore, for $1 \leq i \leq n-1$, α^i is a root of $g_{(q,m,\delta)}^-(x)$ if and only if the sequence of i has a circular run of length at least r with respect to $q-1$. The following proposition presents the degree of $g_{(q,m,\delta)}^+(x)$ and $g_{(q,m,\delta)}^-(x)$.

Proposition 6. [18, p. 155] *Set $r = m - \lambda$. Then*

$$\deg(g_{(q,m,\delta)}^+(x)) = \deg(g_{(q,m,\delta)}^-(x)) = l_r(m) - 1 + (q-1)^2 \sum_{u=0}^{r-2} (r-u-1)(q^{m-r-u-2} - l_r(m-r-u-2)).$$

We have the following estimation on the dimension of $\overline{C}_{(q,m,\delta)}$.

Theorem 7. *Set $r = m - \lambda$. The dimension k of $\overline{C}_{(q,m,\delta)}$ satisfies*

$$k \geq q^m - 2l_r(m) + 2l_r(m-r) - 2(q-1)^2 \sum_{u=0}^{r-2} (r-u-1)(q^{m-r-u-2} - l_r(m-r-u-2)),$$

and

$$k \leq q^m - 2l_r(m) + ml_r(m-r) - 2(q-1)^2 \sum_{u=0}^{r-2} (r-u-1)(q^{m-r-u-2} - l_r(m-r-u-2)).$$

Proof: Since $\lambda \geq \frac{m}{2}$, we have $m \geq 2r$. Define a set $N = \{1 \leq i \leq n-1 \mid g_{(q,m,\delta)}^+(\alpha^i) = g_{(q,m,\delta)}^-(\alpha^i) = 0\}$. Since $\overline{g}_{(q,m,\delta)}(x) = \text{lcm}(g_{(q,m,\delta)}^-(x), x-1, g_{(q,m,\delta)}^+(x))$, we have

$$\deg(\overline{g}_{(q,m,\delta)}(x)) = \deg(g_{(q,m,\delta)}^+(x)) + \deg(g_{(q,m,\delta)}^-(x)) + 1 - |N|.$$

Since $\deg(g_{(q,m,\delta)}^+(x))$ and $\deg(g_{(q,m,\delta)}^-(x))$ are known by Proposition 6, it suffices to estimate the size of N . N contains the number $1 \leq i \leq n-1$, such that \bar{i} contains two runs of length r with respect to 0 and $q-1$, where at most one of them is a circular run. Let N' be the set of integers $1 \leq i \leq n-2$ such that the first r entries of \bar{i} is a straight run of length r with respect to 0 and the last $m-r$ entries contain a

straight run of length r with respect to $q-1$. Clearly, we have $|N'| = l_r(m-r)$. Note that each element of N is a proper cyclic shift of an element of N' . Moreover, for each $i \in N'$, we have

$$2 \leq |\{q^j i \bmod n \mid 0 \leq j \leq m-1\}| \leq m, \quad (2)$$

which implies

$$2|N'| \leq |N| \leq m|N'|.$$

Thus, the conclusion follows from a direct computation. \blacksquare

III. THE MINIMUM DISTANCE OF THE REVERSIBLE BCH CODES $\overline{C}_{(q,m,\delta)}$

While it is difficult to determine the dimension of reversible BCH codes in general, it is more difficult to find out the minimum distance of reversible BCH codes [8]. For the code $\overline{C}_{(q,m,\delta)}$, the BCH bound $d \geq 2\delta$ is usually very tight. But it would be better if we can determine the minimum distance exactly. In this section, we determine the minimum distance d of the code $\overline{C}_{(q,m,\delta)}$ in some special cases.

Given a codeword $c = (c_0, c_1, \dots, c_{n-1}) \in C_{(q,m,\delta)}$, we say c is reversible if $(c_{n-1}, c_{n-2}, \dots, c_0) \in C_{(q,m,\delta)}$. Namely, $c \in C_{(q,m,\delta)}$ is reversible if and only if $c \in \tilde{C}_{(q,m,\delta)}$. The following theorem says that the reversible codeword in $C_{(q,m,\delta)}$ provides some information on the minimum distance on $\overline{C}_{(q,m,\delta)}$.

Theorem 8. *Let $c(x) \in C_{(q,m,\delta)}$ be a reversible codeword of weight w . If $c(1) \neq 0$, then $\overline{C}_{(q,m,\delta)}$ contains a codeword $(x-1)c(x)$ whose weight is at most $2w$. Therefore the minimum distance d of $\overline{C}_{(q,m,\delta)}$ satisfies $d \leq 2w$. In particular, if the weight of $c(x)$ is δ , then the minimum distance $d = 2\delta$.*

Proof: Since $c(x)$ is reversible and $c(1) \neq 0$, we have $(x-1)c(x) \in \overline{C}_{(q,m,\delta)}$. The weight of $(x-1)c(x)$ is at most $2w$, which implies $d \leq 2w$. In particular, if $w = \delta$, together with the BCH bound, we have $d = 2\delta$. \blacksquare

Let $c(x) = \sum_{i=0}^{n-1} c_i x^i$ be a codeword of a cyclic code C with length $n = q^m - 1$. We can use the elements of $\text{GF}(q^m)^*$ to index the coefficients of $c(x)$. Similarly, let \overline{C} be the extended cyclic code of C and let $\overline{c}(x) = \sum_{i=0}^n \overline{c}_i x^i$ be a codeword of \overline{C} with length q^m . We can use the elements of $\text{GF}(q^m)$ to index the coefficients of $\overline{c}(x)$. The support of $c(x)$ (resp. $\overline{c}(x)$) is defined to be the set of elements in $\text{GF}(q^m)^*$ (resp. $\text{GF}(q^m)$), which correspond to the nonzero coefficients of $c(x)$ (resp. $\overline{c}(x)$).

Given a prime power q and an integer $0 \leq s \leq q^m - 1$, s has a unique q -ary expansion $s = \sum_{i=0}^{m-1} s_i q^i$. The q -weight of s is defined to be $wt_q(s) = \sum_{i=0}^{m-1} s_i$. Suppose H is a subset of $\text{GF}(q)^*$, then we use $H^{(-1)}$ to denote the subset $\{h^{-1} \mid h \in H\}$.

The following are two classes of reversible BCH codes whose minimum distances are known.

Corollary 9. *For the reversible BCH code $\overline{C}_{(q,m,\delta)}$, we have $d = 2\delta$ if $\delta \mid n$.*

Proof: It suffices to find a codeword $c(x)$ satisfying the condition in Theorem 8. If $\delta \mid n$, by the proof of [24, Theorem], $C_{(q,m,\delta)}$ contains a reversible codeword $c(x)$ with weight δ , where $c(x) = \sum_{i=0}^{\delta-1} a_i x^{\frac{n}{\delta} i}$ and $c(1) \neq 0$. The desired conclusion then follows from Theorem 8. \blacksquare

Corollary 10. *Let $\delta = 2^r - 1$ and V be an m -dimensional vector space over $\text{GF}(2)$. Suppose $1 \leq r \leq \lfloor \frac{m}{2} \rfloor$, then we can choose four r -dimensional subspaces of V , say H_i , $1 \leq i \leq 4$ of V , such that $H_1 \cap H_2 = \{0\}$ and $H_3 \cap H_4 = \{0\}$. If $((H_1 \cup H_2) \setminus \{0\})^{(-1)} = (H_3 \cup H_4) \setminus \{0\}$, then the reversible BCH code $\overline{C}_{(2,m,\delta)}$ has minimum distance $d = 2\delta$.*

Proof: Define $C_{(2,m,\delta)}^+$ (resp. $C_{(2,m,\delta)}^-$) to be the BCH code with length n and generator polynomial $g_{(2,m,\delta)}^+(x)$ (resp. $g_{(2,m,\delta)}^-(x)$). Let α be a primitive element of $\text{GF}(2^m)$. We can assume the zeros of $C_{(2,m,\delta)}^+$ (resp. $C_{(2,m,\delta)}^-$) include the elements $\{\alpha^i \mid 1 \leq i \leq \delta-1\}$ (resp. $\{\alpha^{-i} \mid 1 \leq i \leq \delta-1\}$).

The BCH code $C_{(2,m,\delta)}^+$ (resp. $C_{(2,m,\delta)}^-$) contains a punctured Reed-Muller code $\text{RM}^+(m-r, m)^*$ (resp. $\text{RM}^-(m-r, m)^*$) as a subcode, in which $\text{RM}^+(m-r, m)^*$ has zeros

$$\{\alpha^i \mid 0 < i < 2^m - 1, wt_2(i) < r\}$$

IV. THE PARAMETERS OF THE REVERSIBLE CODE $\overline{C}_{(q,m,\delta)}$ FOR SMALL δ

In this section, we determine the parameters of the code $\overline{C}_{(q,m,\delta)}$ for a few small values of δ . With the help of Theorem 4 and Corollary 9, we can achieve this in some cases.

Recall that the Melas code over $\text{GF}(q)$ is a cyclic code with length $n = q^m - 1$ and generator polynomial $m_{-1}(x)m_1(x)$ and was first studied by Melas for the case $q = 2$ [21]. The weight distribution of the Melas code has been obtained for $q = 2, 3$ [14], [22]. For $\delta = 2$, the code $\overline{C}_{(q,m,\delta)}$ is the even-like subcode of the Melas code. The following theorem is a direct consequence of Theorem 4 and Corollary 9.

Theorem 11. *Suppose q is odd and $m \geq 2$, then $\overline{C}_{(q,m,2)}$ has parameters $[q^m - 1, q^m - 2 - 2m, 4]$.*

When $\delta = 3$, we have the following result.

Theorem 12. 1) *When $q = 2$ and $m \geq 4$, $\overline{C}_{(q,m,3)}$ has parameters $[2^m - 1, 2^m - 2 - 2m, 6]$.*

2) *When $q^m \equiv 1 \pmod{3}$ and $m \geq 4$, $\overline{C}_{(q,m,3)}$ has parameters $[q^m - 1, q^m - 2 - 4m, 6]$.*

Proof: 1) The dimension follows from Theorem 4. Applying the BCH and the sphere packing bound, we can see that the minimum distance is 6.

2) The dimension follows from Theorem 4. Since $q^m \equiv 1 \pmod{3}$, we have $3 \mid n$. Therefore, by Corollary 9, the minimum distance is 6. ■

Theorem 13. *Suppose $m \geq 3$, then $\overline{C}_{(3,m,4)}$ has parameters $[3^m - 1, 3^m - 2 - 4m, d]$, where $d = 8$ if m is even and $d \geq 8$ if m is odd.*

Proof: It follows from Theorem 4 that the dimension of this code is equal to $q^m - 2 - 4m$. By the BCH bound, the minimum distance of $\overline{C}_{(3,m,4)}$ is at least 8.

When m is even, 4 divides n . Hence, the minimum distance of $\overline{C}_{(3,m,4)}$ is equal to 8 according to Corollary 9. ■

We have the following conjecture concerning the case $q = 3$.

Conjecture 2. *When $\delta = 4$, $m \geq 3$ is odd, and $q = 3$, $\overline{C}_{(q,m,\delta)}$ has minimum distance $d = 8$.*

Example 2. *Let $m = 3$ and $q = 3$. Let α be a generator of $\text{GF}(3^3)^*$ with $\alpha^3 - \alpha + 1 = 0$. Then $\overline{C}_{(q,m,\delta)}$ has parameters $[26, 13, 8]$ and generator polynomial*

$$x^{13} + x^{12} + 2x^{11} + 2x^{10} + x^8 + 2x^5 + x^3 + x^2 + 2x + 2.$$

This is the best ternary cyclic code and has the same parameters as the best linear code with the same length and dimension.

V. CONCLUDING REMARKS

In this paper, we determined the dimension of the reversible BCH code $\overline{C}_{(q,m,\delta)}$ when δ is relatively small, and developed lower and upper bounds on its dimension for $\delta = q^\lambda$, where $\frac{m}{2} \leq \lambda \leq m - 1$. We determined the minimum distance of $\overline{C}_{(q,m,\delta)}$ in two special cases. Moreover, we settled the parameters of the code $\overline{C}_{(q,m,\delta)}$ for some very small δ .

However, the parameters of the reversible BCH codes $\overline{C}_{(q,m,\delta)}$ are still open in most cases. It would be nice if further progress on the determination of the parameters of the codes $\overline{C}_{(q,m,\delta)}$ can be made. According to the tables of best cyclic codes documented in [10], the binary reversible BCH code $\overline{C}_{(q,m,\delta)}$ is the best possible cyclic code in almost all cases (see Table II). Hence, it is worthwhile to study the code $\overline{C}_{(q,m,\delta)}$.

TABLE II
EXAMPLES OF BINARY REVERSIBLE BCH CODE $\overline{C}_{(2,m,\delta)}$

m	n	k	d	δ	Best cyclic?	Optimal?
4	15	6	6	3	Yes	Yes
4	15	2	10	5	Yes	Yes
5	31	20	6	3	Yes	Yes
5	31	10	10	5	No	No
6	63	50	6	3	Yes	Yes
6	63	38	10	5	Yes	Unknown
6	63	26	14	7	Yes	No
6	63	20	18	9	Yes	Unknown
6	63	14	22	11	Yes	No
6	63	2	42	13	Yes	Yes

REFERENCES

- [1] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, 2007.
- [2] E.F. Assmus and J. D. Key, *Designs and Their Codes*, Cambridge University Press, Cambridge, 1992.
- [3] D. Augot, P. Charpin and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 960–973, 1992.
- [4] D. Augot and N. Sendrier, "Idempotents and the BCH bound," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 204–207, 1994.
- [5] E. R. Berlekamp, "The enumeration of information symbols in BCH codes," *Bell System Tech. J.*, vol. 46, no. 8, pp. 1861–1880, 1967.
- [6] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," in: R. Pinto et al. (eds.), *Coding Theory and Applications*, CIM Series in Mathematical Sciences 3, pp. 97–105, Springer, 2015.
- [7] P. Charpin, "On a class of primitive BCH-codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 222–228, 1990.
- [8] P. Charpin, "Open problems on cyclic codes," In: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, vol. I, pp. 963–1063 (Chapter 11), Elsevier, Amsterdam, 1998.
- [9] Y. Dianwu and H. Zhengming, "On the dimension and minimum distance of BCH codes over $GF(q)$," *J. of Electronics*, vol. 13, no. 3, pp. 216–221, July 1996.
- [10] C. Ding, *Codes from Difference Sets*, World Scientific, Singapore, 2015.
- [11] C. Ding, X. Du and Z. Zhou, "The Bose and minimum distance of a class of BCH codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2351–2356, 2015.
- [12] C. Ding, "Parameters of several classes of BCH codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5322–5330, 2015.
- [13] M. Esmaili and S. Yari, "On complementary-dual quasi-cyclic codes," *Finite Fields and Their Applications*, vol. 15, pp. 375–386, 2009.
- [14] G. van der Geer, R. Schoof, and M. van der Vlugt, "Weight formulas for the ternary Melas codes," *Mathematics of Computation*, vol. 58, no. 198, pp. 781–792, 1992.
- [15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [16] T. Kasami and S. Lin, "Some results on the minimum weight of primitive BCH codes", *IEEE Trans. Inf. Theory*, vol. 18, no. 6, pp. 824–825, 1972.
- [17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
- [18] H. B. Mann, "On the number of information symbols in Bose-Chaudhuri codes," *Information and Control*, vol. 5, no. 2, pp. 153–162, 1962.
- [19] J. L. Massey, "Reversible codes," *Information and Control*, vol. 7, no. 3, pp. 369–380, 1964.
- [20] J. L. Massey, "Linear codes with complementary duals," *Discret. Math.* vol. 106-107, pp. 337–342, 1992.
- [21] C. M. Melas, "A cyclic code for double error correction," *IBM J. Res. Develop.*, vol. 4, pp. 364–366, 1960.
- [22] R. Schroof and M. van der Vlugt, "Hecke operators and the weight distribution of certain codes," *J. Comb. Theory Ser. A*, vol. 57, pp. 163–186, 1991.
- [23] N. Sendrier, "Linear codes with complementary duals meet the Gilbert-Varshamov bound," *Discret. Math.*, vol. 285, pp. 345–347, 2004.
- [24] K. K. Tzeng and C. R. P. Hartmann, "On the minimum distance of certain reversible cyclic codes", *IEEE Trans. Inf. Theory*, vol. 16, no. 5, pp. 644–646, 1970.
- [25] D. Yue and G. Feng, "Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2625–2628, 2000.